

APPARATUS AND METHOD FOR COMMUNICATION FOR MAKING DATA SAFE

Publication number: JP2002319936 (A)

Publication date: 2002-10-31

Inventor(s): SUZUKI TAKASHI; YOSHIMURA TAKESHI + (SUZUKI TAKASHI, ; YOSHIMURA TAKESHI)

Applicant(s): NTT DOCOMO INC + (NTT DOCOMO INC)

Classification:

- international: G09C1/00; H04L12/22; H04L12/56; H04L29/06; H04L9/36; G09C1/00; H04L12/22; H04L12/56; H04L29/06; H04L9/36; (IPC1-7): G09C1/00; H04L12/22; H04L12/56; H04L9/36

- European: H04L29/06; H04L29/06512A; H04L29/06516E; H04L29/0654B

Application number: JP20010122610 20010420

Priority number(s): JP20010122610 20010420

Abstract of JP 2002319936 (A)

Translate this text

PROBLEM TO BE SOLVED: To enable header compression in the case of mobile communication by selectively encrypting data and generally applying them to an application on a UDP. **SOLUTION:** Each of parameters indicating encryption except for a header together with an encryption algorithm or the like is shared with opposite apparatus by communication by a parameter sharing part 34 and while using the shared parameter, an identifier for data identification to an entire RTP packet from an application part 31 is calculated by an encryption/identifier adding part 33. Then, the identifier is added to the RTP packet and the data of a part except the header are encrypted and outputted to a transport part 32. In this transport part, a UDP header is added to a non-enciphered RTP header and a UDP packet is generated and sent to a network part 35.

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-319936

(P2002-319936A)

(43)公開日 平成14年10月31日(2002.10.31)

(51) Int.Cl. [*]	識別記号	F I	フジタ(参考)
H 04 L 9/36		G 09 C 1/00	6 4 0 D 5 J 1 0 4
G 09 C 1/00	6 4 0	H 04 L 12/22	5 K 0 3 0
H 04 L 12/22		12/56	3 0 0 A
12/56	3 0 0	9/00	6 8 5

審査請求 未請求 請求項の数15 O.L. (全 10 頁)

(21)出願番号 特願2001-122610(P2001-122610)

(71)出願人 392026693

株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目11番1号

(22)出願日 平成13年4月20日(2001.4.20)

(72)発明者 鈴木 敏
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内(23)発明者 吉村 健
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内(74)代理人 100068153
弁理士 草野 卓 (外1名)

Fターム(参考) 5J104 AA08 AA33 LA01 PA07

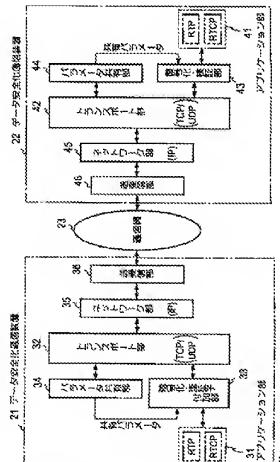
SK030 GA15 HA08 JA05 LD18

(54)【発明の名称】 データ安全化通信装置及びその方法

(57)【要約】

【課題】 選択的に暗号化し、かつUDP上のアプリケーションに汎用的に適用でき、移動通信におけるヘッダ圧縮を可能とする。

【解決手段】 パラメータ共有部3.4により暗号化アルゴリズムなどと共にヘッダを除く暗号化であることを示す各パラメータを相手装置と通信により共有し、その共有したパラメータを用いて、暗号化・認証子付加部3.3でアプリケーション部3.1からのRTPパケット全体に対するデータ認証のための認証子を計算し、その認証子をRTPパケットに付加し、そのヘッダを除いた部分を暗号化してトランsport部3.2へ出力し、ここでUDPヘッダを前記非暗号化RTPヘッダに付けてUDPパケットを作りネットワーク部3.5へ送出する。



【特許請求の範囲】

【請求項1】 通信路を介して入力データの安全化対象を示すパラメータを相手のデータ安全通信装置と共有するパラメータ共有手段と、前記共有されたパラメータに従って前記入力データの一部を選択的に安全化して出力する安全化手段とを備えたことを特徴とするデータ安全化通信装置。

【請求項2】 請求項1に記載の装置において、入力データの種別(アプリケーション)に応じて上記安全化対象を決定する手段を備えたことを特徴とするデータ安全化通信装置。

【請求項3】 請求項1または2に記載の装置において、この装置が接続された網の伝送特性に応じて上記安全化対象を決定する手段を備えたことを特徴とするデータ安全化通信装置。

【請求項4】 請求項1乃至3の何れかに記載の装置において、

前記安全化対象は暗号化対象であり、前記相手のデータ安全化通信装置は暗号復号化装置であり、前記安全化手段は暗号化手段であることを特徴とするデータ安全化通信装置。

【請求項5】 請求項4に記載の装置において、前記入力データはRTPパケットであり、前記暗号化対象はRTPヘッダを除くデータであることとを特徴とするデータ安全化通信装置。

【請求項6】 請求項4に記載の装置において、前記暗号化対象を決定する基準は、前記網の通信路の伝送速度であることを特徴とするデータ安全化通信装置。

【請求項7】 請求項1乃至3の何れかに記載の装置において、

前記安全化対象は前記入力データの認証処理範囲であり、前記相手のデータ安全化通信装置はデータ検証装置であり、前記安全化手段は前記入力データのうち前記認証処理範囲から認証子を計算する手段であり、入力データに前記認証子を付加して出力する手段とを含むことを特徴とするデータ安全化通信装置。

【請求項8】 通信路を介して受信データの暗号復号化対象を示すパラメータを相手のデータ安全化装置と共有する手段と、受信データのうち、前記共有されたパラメータに従って一部を選択的に復号化する暗号復号化手段と、を備えることを特徴とするデータ安全化通信装置。

【請求項9】 通信路を介して受信データの認証範囲を示すパラメータを、相手の認証子付加装置と共有する手段と、

受信データのうち前記パラメータに従って前記認証範囲のデータと前記受信データに含まれる認証子から前記認証範囲に含まれるデータの正当性を検証する検証手段

と、を具備することを特徴とするデータ安全化通信装置。

【請求項10】 通信路を介して入力データの暗号化対象を示すパラメータを相手暗号復号化装置と共有する過程と、

前記共有したパラメータに従って前記入力データの一部を選択的に暗号化して出力する過程とを有するデータ安全化通信方法。

【請求項11】 請求項10に記載の方法であって、前記入力データはRTPパケットであり、

前記選択的暗号化を、前記RTPパケットのRTPヘッダを除くデータに対して行うことを特徴とするデータ安全化通信方法。

【請求項12】 通信路を介して入力データの認証処理範囲を示すパラメータをデータ検証装置と共有する過程と、

前記入力データのうち前記パラメータで指定された部分から認証子を計算する過程と、

前記入力データに前記認証子を付加して出力する過程とを有するデータ安全化通信方法。

【請求項13】 通信路を介して受信データの暗号復号化対象を示すパラメータを相手の暗号化装置と共有する過程と、

受信データのうち、前記共有されたパラメータに従って一部を選択的に暗号復号化する過程とを有することを特徴とするデータ安全化通信方法。

【請求項14】 請求項13に記載の方法において、前記受信データはRTPパケットであり、前記選択的暗号復号化を、前記RTPパケットのRTPヘッダを除くデータに対して行うことを特徴とするデータ安全化通信方法。

【請求項15】 通信路を介して受信データの認証範囲を示すパラメータを、相手の認証子付加装置と共有する過程と、

受信データのうち前記パラメータに従って前記認証範囲のデータと前記受信データに含まれる認証子から前記認証範囲に含まれるデータの正当性を検証する過程とを有することを特徴とするデータ安全化通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、伝送データの傍受、改変などに対するデータの安全化、つまり暗号化、データ認証を行う通信機能及びその方法に関する。

【0002】

【従来の技術】インターネットに代表されるIP(インターネットプロトコル)ネットワークには本来セキュリティ機能が備わっていない。何ら対策を施さない場合、途中経路におけるIPパケットの取得や改変などにより、通信の当事者に知られずに通信内容の傍受、改変が可能である。このため、IPネットワーク上で商取引な

どの重要な情報を送受信する場合には、いかにセキュリティ（安全性）を保つかが重要な課題となる。

【0003】例えは、音楽や映像をインターネット経由で配信するコンテンツ配信サービスでは、配信される音楽・映像データが価値をもった重要な情報となり、途中経路における傍聴、変容を防ぐ必要がある。また、IPネットワークを介して電話サービスを提供するVoIPシステムにおいては、通話内容の不法な傍聴を防ぐ必要がある。VoIPシステムやストリーム型コンテンツ配信システムにおいては、リアルタイム性（実時間性）が要求されるデータを伝送するために、RTP／UDPが一般的に利用されている。RTP（Realtime Transport Protocol）はアプリケーション層で用いられるプロトコルであり、実時間処理に適する。UDP（User Datagram Protocol）はアプリケーション層とネットワーク層とのインターフェースであるトランsport層に用いられるコネクションレスプロトコルである。RTP／UDPでは、TCP（Transmission Control Protocol）、トランsport層で用いられるコネクション型プロトコル）のようにパケットの確実な送達よりも、即時性のあるパケットの送達を目指しているため、途中経路でパケットロス（紛失）が生じる可能性がある。このため、RTP／UDPに適用するセキュリティ技術を検討する際に、パケットロスに対する対策が必要となる。

【0004】また、現在急速に普及している移動通信への適用も重要な課題である。移動通信網にてRTP／UDPパケット伝送を行う際には、無線伝送帯域の利用効率改善のために、無線リンクにおいてRTPパケット及びUDPパケットの両ヘッダは対ヘッド圧縮が適用される。従って、セキュリティ技術、特に暗号化方式を検討する際にも途中的リンクにおけるRTP／UDPパケットのヘッダ圧縮が可能である方式が望まれる。移動通信網への適用を前提としたRTPパケットのセキュア（安全）な伝送方式として、IETF（インターネット標準化推進団体）においてSecure RTP（SRTP、参照：draft-ietf-avt-srtp-00.txt）が提案されている。SRTPでは、ヘッダ圧縮を適用可能とするための選択的暗号化やパケットロスやビット誤りの影響が少ない暗号化方式などが導入されている。つまりRTPヘッダに対して、RTPペイロードの部分だけを暗号化し、この暗号化されたRTPペイロードとRTPヘッダに対して、データ認証コード（認証子）を生成し、これを付加して、RTPヘッダと暗号化RTPペイロードのデータの正当性を検証可能にしている。このため、効率的な保護が可能であるが、その一方RTPに特化した技術となっている。つまりSecure RTPを使用する場合は図12Bに示すように、RTPに特化した暗号化アルゴリズム暗号化パラメータが用いられるため、他のUDP上のアプリケーション、トランsportプロトコルにそのSecure

e RTPを用いることはできない。選択的暗号化パラメータ、暗号化アルゴリズムが固定であり、新規プロトコルに対応できない他の技術進歩の早いコンテンツ配信には適さない。このようにあるるアプリケーションに特化したセキュリティ技術は、新規アプリケーションが開発される度に個別のセキュリティ技術を検討する必要があり、好ましくない。また、安全性技術は永久的ではないためSecure RTPは暗号化アルゴリズムなども固定であり、セキュリティ上問題がある。

【0005】一方、インターネットで広く利用されているセキュリティ技術としてSSL（Secure Socket Layer）（TLS）がある。つまりSSL（TLS）を使用しない状態では図13Aに示すようにアプリケーション層におけるHTTP（Hypertext Transfer Protocol）、FTP（File Transfer Protocol）、Telnet（遠隔ログイン）などのアプリケーション層とTCP又はUDPのトランsport層が直接接続される。図13Bに示すようにSSLは、TCPやUDPなどのトランsport層とアプリケーション層との間に位置するセキュリティプロトコルである。SSLは、TCPやUDPが提供するデータ伝送機能を利用して送受信されるデータに何らかのセキュリティ処理を施すことで、アプリケーション層に対してセキュアなデータ伝送サービスを提供する。このため、利用できるアプリケーション、暗号化アルゴリズムが限定されないという特徴を備える。SSLは、特にWebアクセスで使用されるHTTPセッションを保護するために広く用いられているが、FTPやTelnetなど他のアプリケーションにも汎用的に利用できる。また、SSLを移動通信網に修正したものとして、WAP Forumで規格化されたWTLSがある。

【0006】SSLやWTLSは、図14に示すように大きく分けて2層構造になっている。この2層中の下位層で使用されるプロトコルはレコードプロトコル（Record Protocol）と呼ばれており、上位層のプロトコルのデータを暗号化する機能およびデータ認証コード（MAC）を附加する機能を提供する。SSLの2層構造中の上位層にはハンドシェークプロトコル（Handshake Protocol）、アラートプロトコル（Alert Protocol）、チャンジサイフプロトコル（Change Cipher Protocol）、アプリケーションデータプロトコル（Application Data Protocol）の4種類が含まれる。ハンドシェークプロトコルは暗号化・データ認証方式のネゴシエーション機能および握手・サーバの認証機能を有し、アラートプロトコルはイベントやエラーの通知機能を有し、チャンジサイフプロトコルはネゴシエーションした暗号化・認証方式を有効にする機能を有する。つまり暗号通信の開始を相手に通知するアプリケーションデータプロトコルは、上位のアプリケーションデータを透過的に送受信するものであり、HTTPやFTPなどのデータはこのプロ

ロトコルを介してレコードプロトコル (Record Protocol) に受け渡される。

【0007】図5に送信側と受信側のレコードプロトコル (Record Protocol) 間で送受信されるデータ構造の例を示す。ヘッダ10には上位プロトコル種別 (ハンドシェーク、アラート、アプリケーションデータなど) を示す識別子 (Protocol type) 11、SSLのバージョン (Major Version, Minor Version) 12、データ長 (Length[high], Length[low]) 13が、ペイロードには暗号化された上位プロトコルのデータ14が含まれている。暗号化データ14はデータ本体 (Content) とこのデータ本体及びヘッダの正当性検証用認証子MACが含まれている。この構造はレコードプロトコルを利用するプロトコル全てに適用されるものであり、アプリケーションプロトコルも例外ではない。従って、SSLを利用してRTTパケットを伝送する場合には、RTTパケットのヘッダ及びペイロードの全体が暗号化され、レコードプロトコルデータのペイロード14にマッピングされる事となる。

【0008】のように、RTTパケット全体を暗号化したものに、もしくはRTTパケットにレコードプロトコルのヘッダを附加した場合、途中経路におけるRTTパケット圧縮の適用が不可能になる。つまりヘッダ圧縮は、連続して設けられているRTTパケットとUDPヘッダとIPヘッダとを…括して行うため、RTTパケットとUDPヘッダとの間にレコードプロトコルヘッダ10が挿入されると、これらを…括してデータ圧縮することができなくなる。このため、SSL/WTLSをRTTパケットの保護に適用することは、移動通信においては望ましくない。

【0009】

【発明が解決しようとする課題】また一般的のデータの通信においても、特に安全にしたい部分に対してのみ、暗号化や正当性を検証できる認証を付けるなどの安全性を施して通信することができれば、便利であるが、その安全性を適応的に付けることは困難であった。この発明の目的は入力データの一部にのみ選択的に安全性を施して通信することを可能にするデータ安全化通信装置及びその方法を提供することにある。

【0010】

【課題を解決するための手段】この発明によれば、入力データの安全化対象を示すパラメータを相手のデータ安全化通信装置と通信路を介して共有し、この共有されたパラメータに従って入力データの一部を選択的に安全化して出力する。

【0011】

【発明の実施の形態】第1実施形態

図1にこの発明の第1実施形態を示すと共にその実施形態を用いたデータ伝送システムの概要を示す。例えばサーバやデータ端末などのこの発明による送信側のデータ

安全化通信装置21と、同様にサーバやデータ端末などのこの発明による受信側のデータ安全化通信装置22とが通信網23を通じて接続することができる。通信網23は1つの網として示しているが、公衆通信網とインターネット網とが組合された網など、複数網から構成されているてもよい。

【0012】データ安全化通信装置21はアプリケーション部31ヒトランスポート部32との間にこの実施形態では安全化手段として暗号化・認証子付加部33が設けられる。またトランスポート部32の上位層としてパラメータ共有部34が設けられる。トランスポート部32はTCPやUDP機能を有し、例えばIP機能を有するネットワーク部35と接続され、ネットワーク部35は物理層である送受信部36に接続され、送受信部36は通信網23と接続される。データ安全化通信装置22もデータ安全化通信装置21とほぼ同様に構成され、つまりアプリケーション部41、トランスポート部42、ネットワーク部45及び送受信部46を備え、この実施形態では安全化手段として復号化・検証部43が設けられまたトランスポート部42の上位層としてパラメータ共有部44が設けられる。

【0013】通信装置21はアプリケーション部31からのアプリケーションデータの送信に先立ち、データ安全化に必要なパラメータ、つまり暗号化処理・データ認証子(コード)生成処理に必要なパラメータを相手の装置22と交換して、これらのパラメータを相手通信装置22と共有する。このパラメータの例えは図2に示すように暗号化アルゴリズムを、Null、DES、3DES、RC4などの何れにするか、データ認証子生成アルゴリズムをMD5、SHAなどの何れにするか、鍵を生成するために用いる秘密情報、通信装置21(例えはサーバ側鍵)及び通信装置22(例えはクライアント側鍵)における暗号化・復号化あるいは認証・検証に用いるランダム値、送信データ中の暗号化する範囲、データ認証する範囲などである。この実施形態では特にこの共有するパラメータとして暗号化範囲及びデータ認証範囲を新たに設けた点が重要であり、他のパラメータを共有することは、従来のSSL(TSL)による安全化プロトコルで用いられる共有パラメータと同様のものであり、またこれらパラメータの共有は、従来のSSLと同様に通信路を介して、通信装置21と22が相互に通信して行う。

【0014】ここで新たに用いる共有パラメータである、伝送すべきデータの安全化対象を示すパラメータ、この例では暗号化範囲及びデータ認証範囲は、入力データパケット(この例ではアプリケーション部31よりのデータパケット)のどの範囲を暗号化、認証するかを決定するための情報であり、様々な指定方法が考えられるが、例えは「パケット先頭の何バイト目から暗号化を開始する」などにより指定する。更にこの暗号化範囲、デ

ータ認証範囲の決定は入力データの種別、つまりこの例ではアプリケーションに応じて、あるいは通信装置21が接続された通信網23の伝送特性（伝送速度、選択特性、伝送誤り特性、減衰特性、周波数特性、歪特性など）に決定される。

【0015】通信装置21のパラメータ共有部34では、例えば図3に示す手順により安全化対象を示すパラメータを共有決定する。暗号化通信要求を受信すると(S1)、入力データアプリケーションパケットがRTPパケットであるかを調べ(S2)、RTPパケットであれば、装置21が接続されている通信網23が伝送速度が低い網、例えば移動通信網であるかを調べ(S3)、移動通信網であれば、RTPパケットを選択的に暗号化すると、例えば入力データ先頭のRTPヘッダを暗号化対象外とすることを示す暗号化・認証パラメータを相手通信装置22へ送信する(S4)。なおこの際に暗号化アルゴリズム、データ認証子生成アルゴリズムなど他のパラメータも送信する。

【0016】一方相手通信装置22のパラメータ共有部44では例えば図4に示すように通信装置21から暗号化・認証パラメータを受信すると(S1)、受信した通信相手の暗号化・認証パラメータがRTPパケット選択的暗号化であるかを調べ(S2)、そうであれば、パラメータ共有部44における暗号化・認証パラメータをRTPパケット選択的暗号化に決定し(S3)、その決定した暗号化・認証パラメータを通信装置21へ送信する(S4)。通信装置21のパラメータ共有部34では、図3に示すように通信装置22からRTPパケット選択的暗号化を示す暗号化・認証パラメータを受信すると(S5)、暗号化・認証パラメータをRTPパケット選択的暗号化に決定する(S6)。このようにして両パラメータ共有部34、44において暗号化・認証パラメータとしてRTPパケット選択的暗号化が通信路を介して共有される。なお暗号化アルゴリズムなどの他のパラメータも同様にして同時に決定される。この場合、例えば従来のSSLなどと同様に、各パラメータについていくつかの候補を送って、相手装置22により決定してもらう。

【0017】図3において、ステップS2で入力データがRTPパケットでないと判定され、あるいはステップS3で通信装置21が接続されている通信網23の伝送速度が高いと判定された場合は、この例では入力データ（パケット）全体を暗号化する。つまり非選択的暗号化を示す暗号化・認証パラメータを相手通信装置22へ送信する(S7)。通信装置22のパラメータ共有部44では図4に示すように、ステップS2で受信した通信相手の暗号化・認証パラメータがRTPパケット選択的暗号化でないと判定されると、通信装置22のアプリケーション部41からの入力データ（アプリケーション）がRTPパケットであるかを判断し(S5)、RTPパケ

ットであれば、通信装置22が接続された通信網23が伝送速度の低い、例えば移動通信網であるかを調べ(S6)、そうであれば、ステップS3に移り、RTPパケット選択的暗号化を表わす暗号化・認証パラメータを決定して、これを通信装置21へ送信する(S4)。ステップS5で入力データがRTPパケットではないと判定され、あるいはステップS6で接続されている通信網23の伝送速度が低くない移動通信網ではないと判定される(S6)、非選択的暗号化を表わす暗号化・認証パラメータを決定して(S7)、相手通信装置21へ送信する(S4)。

【0018】通信装置21のパラメータ共有部34では、図3に示すように、ステップS7の送信後、相手通信装置22から暗号化・認証パラメータを受信すると(S8)、その受信暗号化・認証パラメータがRTPパケット選択的暗号化であるかを調べ(S9)、そうであればステップS6に移り、暗号化・認証パラメータを、RTPパケット選択的暗号化に決定し、RTPパケット選択的暗号化でなければ暗号化・認証パラメータを非選択的暗号化に決定する(S10)。このようにしてパラメータ共有部34と44は通信路を介して暗号化範囲を共有することができる。認証範囲は入力データ（アプリケーション）にかかわらず、また通信装置21、22がそれぞれ接続されている通信網23の伝送特性に係わらず、入力データの全体とする。暗号化範囲としてはヘッダを除くか部分のみならず、暗号化範囲、認証範囲としては入力データが画像や音声である場合に、その重要な部のみとすることができる。この場合、例えばこれらデータの符号化の際に欠落すると復号が不可能となる重要なコードのみを自動的に暗号化するように指示することもできる。何れの場合も、暗号化アルゴリズムなど他のパラメータも、前記暗号化範囲の共有と同時に共有する処理を行つる。

【0019】以上のようにしてパラメータが共有されるると、共有された各種パラメータはパラメータ共有部34、44からそれぞれ暗号化・認証子付加部33、復号化・検証部43へ供給される。暗号化・認証子付加部33において暗号化・認証子付加の処理が行われる。その手順の例を図5に示す。上位アプリケーション部31からデータパケットが入力されると(S1)、アプリケーションデータプロトコルにより、透過的に暗号化・認証子付加部33に入力され(S2)、このデータパケットのうち認証範囲パラメータに従って選択された部分を用いて共有した認証子生成アルゴリズム・認証子生成用鍵により認証子を生成する(S3)。認証子生成方法は、例えば、今井秀樹著「暗号のおはなし」4、7節に詳しい。例えばハッシュ関数により認証範囲データを圧縮し、圧縮データを共通鍵で暗号化することにより生成する。その後、入力されたデータパケットに認証子を付加し(S4)、この認証子付データパケットに対し、暗号

範囲パラメータに基づいて選択部分の暗号化を共有した暗号アルゴリズム、暗号鍵を用いて施す(S5)。なおプロック暗号化を行う場合は、その固定ブロック長にデータが不足した場合に埋め合せるパディングを暗号化の前に行う(S6)。

【0020】このようにして暗号化されたデータ構造の例を図6に示す。この例では入力されたアプリケーションデータに対し、認証子MACが付加され、アプリケーションデータ中のヘッダを除いた部分(ペイロード)と認証子が暗号化されている。この選択的暗号化を含むデータは下位のトランスポート部32に受け渡され相手通信装置22へ伝送される。受信側通信装置22では、上記の逆の手順を用いて暗号化されたデータを復号し、データ認証子(コード)を利用して受信データの正当性を検証する。つまり図1中の通信装置22において、通信装置21から受信したパケットはトランスポート部4より復号化・検証部43に入力され、復号化・検証部43で共有した暗号化アルゴリズム、暗号化鍵、暗号化範囲に従って、この暗号化された部分が選択的に復号され、この復号されたデータ中のデータ認証子(コード)MACを用いて、ヘッダ及び復号化されたペイロード、つまり図6中のアプリケーションデータの正当性の検証を行なう。正当であれば、このアプリケーションデータをアプリケーション部41へ供給する。

【0021】このように暗号化範囲を共有することにより、入力データ中の一部を選択的に暗号化することができます、例えば安全性が問題になる部分のみを暗号化することにより、全体を暗号化する場合よりも処理量が少なく済み、しかも、安全性が問題になるおそれがない。暗号化範囲は、暗号化のための他のパラメータを共有する処理と同時に行なうことができ、このための処理の増加はわずかである。特に前記例のように入力データ(アプリケーション)がRTPパケットの場合で、そのRTPパケットのヘッダ部分を暗号化しない領域とする場合は、このヘッダにUDPパケットヘッダ、IPパケットヘッダが付加されることになり、Secure RTP同様に、途中経路におけるRTPパケットヘッダを含めたヘッダ圧縮に対応可能である。また、Secure RTPとは異なり、暗号化領域は通信相手との交換によりセッション開始時に既定可能であるため、RTPパケット以外のアプリケーションにも汎用的に対応可能である。

【0022】図7では、認証子付加後に暗号化を行ったが、図7に示すように暗号化後に認証子を生成し、暗号化されたパケットに認証子を付加しても良い。この場合、受信側では、受信データの正当性を検証した後、暗号の復号化を行ふことになる。以上の選択的安全性処理の流れは図8に示すようにデータが入力されると(S1)、入力データの安全化対象を示すパラメータを相手通信装置と通信路を介して共有し(S2)、その共有し

た安全化対象パラメータに従って入力データの一部に対して安全化処理を行って(S3)、相手装置へ送信する(S4)。

第2実施形態

図9にこの発明の第2実施形態を示す。これは図14に示したS5を拡張して選択的暗号化をサポート可能としたものである。第1実施形態におけるパラメータ共有部34はさらに相手通信装置22と認証処理や暗号化・データ認証パラメータを交換するハンドシェーク(Hand shake)部34a、暗号化・データ認証パラメータを有効化するチェンジシффア(Change Cipher)部34b、イベント・エラーを通知するアラート(Alert)部34c、そして、下位レイヤ部32を介して上記3つの各部34a、34b、34cのプロトコルデータを送受信するための第1レコード(Record)部34dからなる。第1レコード部34dのプロトコルデータフォーマットにはSSLのレコード部と同じフォーマットを利用する。シェーカーハンド部34aでは、第1レコード部34bおよび第2レコード部、つまり暗号化・認証子付加部33で利用する暗号化・データ認証パラメータを相手通信装置22と交換して共有する。またチェンジシfffア(Change Cipher)部34bは第1レコード部34dおよび第2レコード部33の暗号化・データ認証パラメータを有効化する。つまりその暗号化を開始させて相手に通知する。第1レコード部34dには、ハンドシェーク部34aのプロトコルメッセージや選択的暗号化が不要なアプリケーションのデータが入力される。

【0023】選択的暗号化が必要なアプリケーションデータの送受信は、上記のプロトコルデータとは別に第2レコード部、つまり暗号化・認証子付加部で送受信される。第2アプリケーションデータ部38は上位の第1アプリケーション部31aのデータパケットを透過的に第2レコード部33に受け渡すためのものである。また、第1レコード部34dと異なり、第2レコード部、つまり暗号化・認証子付加部33では入力データに対して新たなヘッダは追加せず、暗号化・認証子生成処理のみを施す。第1レコード部34dで共有されたパラメータは第2レコード部33の暗号化・データ認証処理に利用される。暗号化・データ認証処理は第1実施形態と同様である。

【0024】パラメータ共有部34のハンドシェーク部34aによる相手通信装置とのパラメータ共有処理は最初は平文で通過を行なうが、途中からは図15に示したデータ構造により、暗号化・認証子付加を行って、これらパラメータの共有に対する安全化してもよい。またアプリケーションでもRTPパケットのように実時間性が要求されない、頻繁に送られないHTTP、FTP、Telnet、RTSP(RTPのセッションを開くためのプロトコル)などのアプリケーションデータパケットは第1アプリケーション部31bより第1アプリケ

ションデータ部37へ通じて第2レコード部34dに入力して、これらに対しては、共有したパラメータにより暗号化をそのパケット全体に対して行い、図15に示したようにレコード部のヘッダ10を付けてレコードプロトコルパケットとしてトランスポート部32へ供給する。なお相手側装置22においては図9中の第2レコード部である暗号化・認証子付加部33が、復号化・検証部になり、他は同様の構成である。

第3実施形態

図10は、この発明の第3実施形態を示す。この実施形態では、R T S PやH T T Pなどの第1アプリケーション部31aを介してR T Pなど第2アプリケーション部31bのアプリケーションデータに対して適用される暗号化・認証子付加パラメータを共有するための通信相手との交渉をする。例えば、図2の暗号化パラメータを相手通信装置22の公開鍵で暗号化して、プロトコルメッセージボディに埋め込むことで相手通信装置22に伝送することができる。

【0025】1つの通信装置に暗号化・認証子付加部と復号化・検証部をもせててもよい。上述においてはデータに対する安全性として暗号化とデータ認証子付加との両者を用いたが、その一方のみを用いてもよい。通信装置21、22の各部をコンピュータにプログラムを実行させて機能させてもよい。

【0026】

【発明の効果】以上説明したように、この発明によればデータの一部を選択的に安全化を施すことができ、かつ特定のアプリケーションに依存しない汎用的な伝送データ保護が可能であり、しかも特に移動通信に適用すればヘッダ圧縮も可能である。

【図面の簡単な説明】

【図1】この発明装置の実施形態の機能構成及びこの発明装置が用いられるシステム構成例を示す図。

【図2】暗号化パラメータの例を示す図。

【図3】送信側における暗号範囲共有処理手順の例を示す流れ図。

【図4】受信側における暗号範囲共有処理手順の例を示す流れ図。

【図5】図1中の暗号化・認証子付加部33の処理手順の例を示す流れ図。

【図6】図1中の暗号化・認証子付加部33の出力パケットのデータ構造の例を示す図。

【図7】暗号化・認証子付加部33の処理手順の他の例を示す流れ図。

【図8】この発明の方法の処理手順の例を示す流れ図。

【図9】この発明装置の第2実施形態の機能構成を示す図。

【図10】この発明装置の第3実施形態の機能構成を示す図。

【図11】選択的暗号化されたパケットのデータ構造を示す図。

【図12】AはS e c u r e R T Pを使用しない処理を示す図、BはS e c u r e R T Pを使用する時の処理を示す図である。

【図13】AはS S L / W T L Sを使用しないアプリケーションデータの処理を示す図、BはS S L / W T L Sを使用する場合の処理を示す図である。

【図14】S S L / W T L Sレイヤの詳細を示す図。

【図15】S S L / W T L Sにより処理されたレコードプロトコルデータの構造を示す図。

【図1】

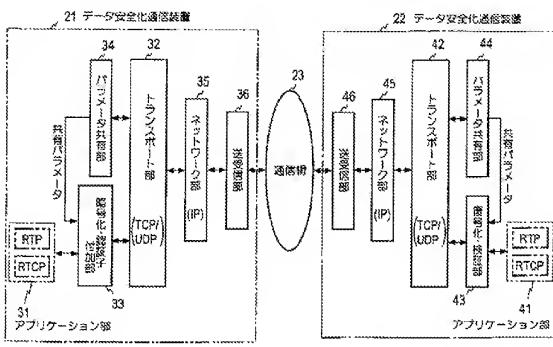
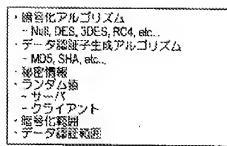


図1

【図2】



【図3】

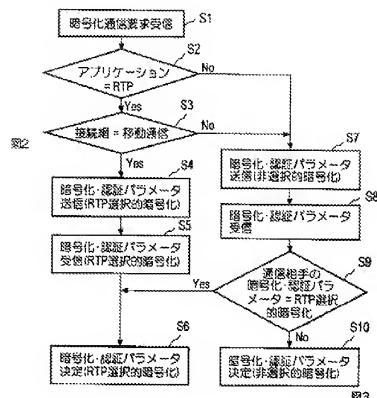


図3

【図4】

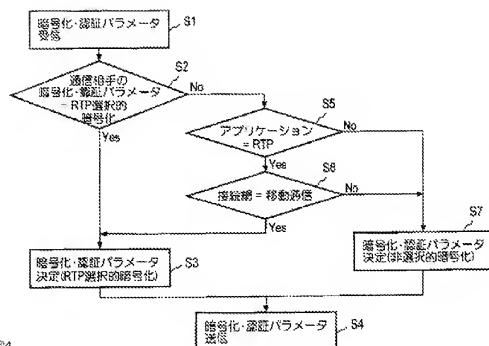


図4

【図8】

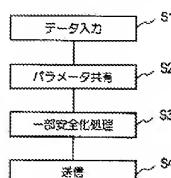


図8

【図6】

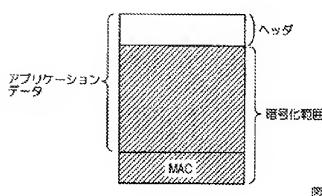


図6

【図11】

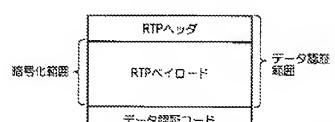
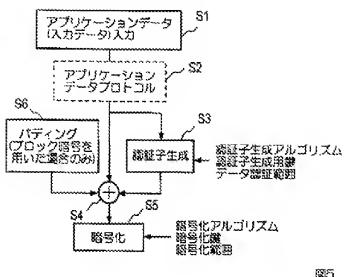
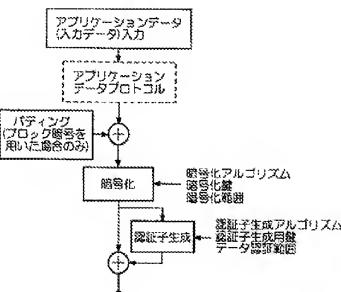


図11

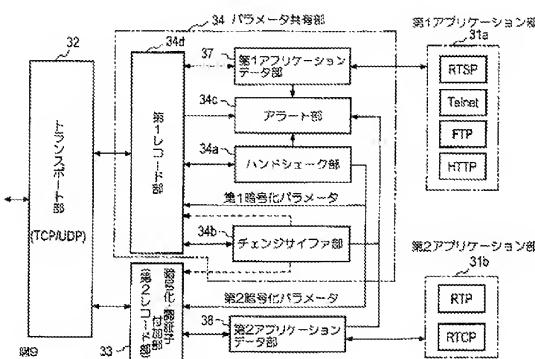
185



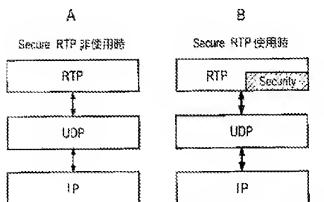
[四七]



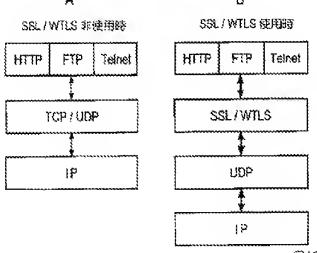
1001



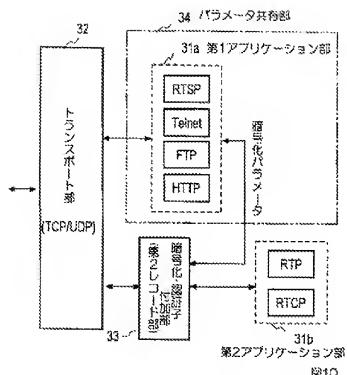
[图1-2]



[图] 13



【図10】



【図14】

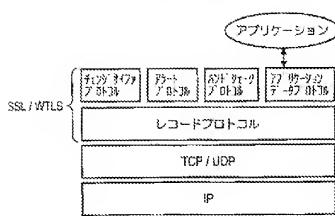


図14

【図15】

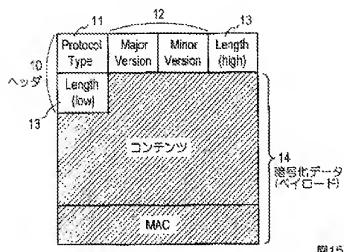


図15



US 20030167394A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0167394 A1
Suzuki et al. (43) Pub. Date: Sep. 4, 2003

(54) DATA SECURING COMMUNICATION APPARATUS AND METHOD

Publication Classification

(76) Inventors: Takashi Suzuki, Lafayette, CA (US);
Takeshi Yoshimura, Kanagawa (JP)(51) Int. Cl.⁷ H04L 9/00
(52) U.S. Cl. 713/168

Correspondence Address:
OBON, SPIVAK, MCCLELLAND, MAIER &
NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314 (US)

(57) ABSTRACT

(21) Appl. No.: 10/333,748

A parameter sharing part 34 performs, by communication, processing for sharing an encryption algorithm and parameters indicative of encryption of data except a header with an apparatus of the other party; an encryption/authenticator adding part 33 calculates the shared parameters an authenticator for data authentication of an RTP packet in its entirety from an application part 31, then adds the authenticator to the RTP packet, then encrypts it except its header, and outputs the packet to a transport part 32; and the transport part adds a UDP header to the said non-encrypted RTP header to form a UDP packet and provides it to a network part 35.

(22) PCT Filed: Apr. 22, 2002

(86) PCT No.: PCT/JP02/03980

(30) Foreign Application Priority Data

Apr. 20, 2001 (JP) 2001-122610

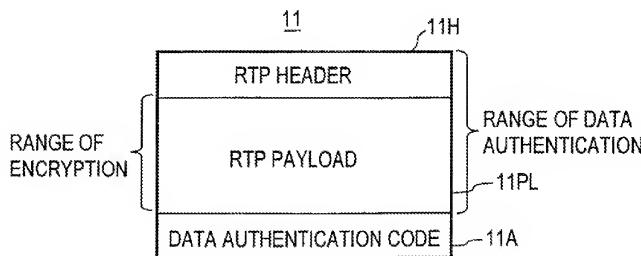


FIG.1A

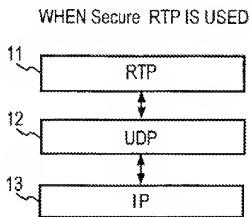


FIG.1B

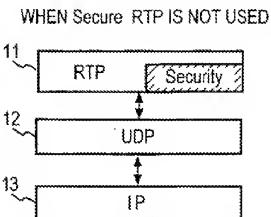


FIG.2

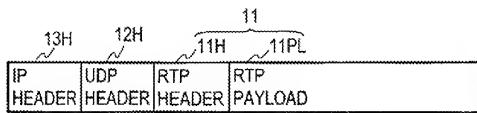


FIG.3

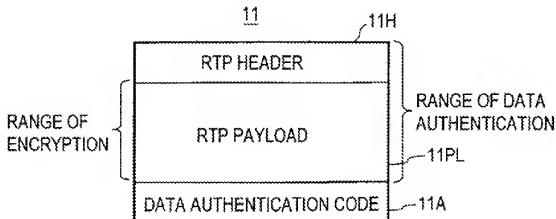


FIG.4A

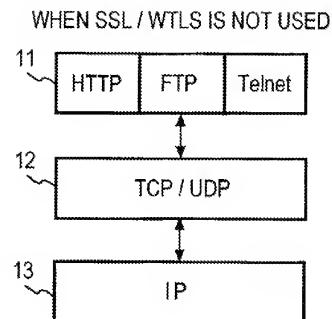


FIG.4B

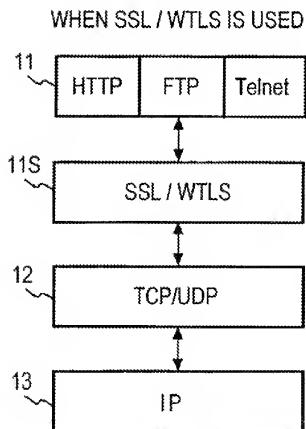


FIG.5

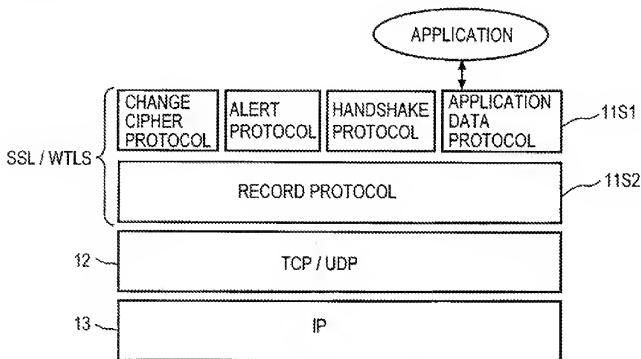


FIG.6

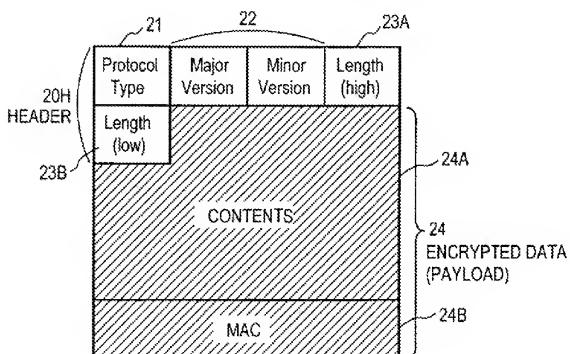


FIG.7

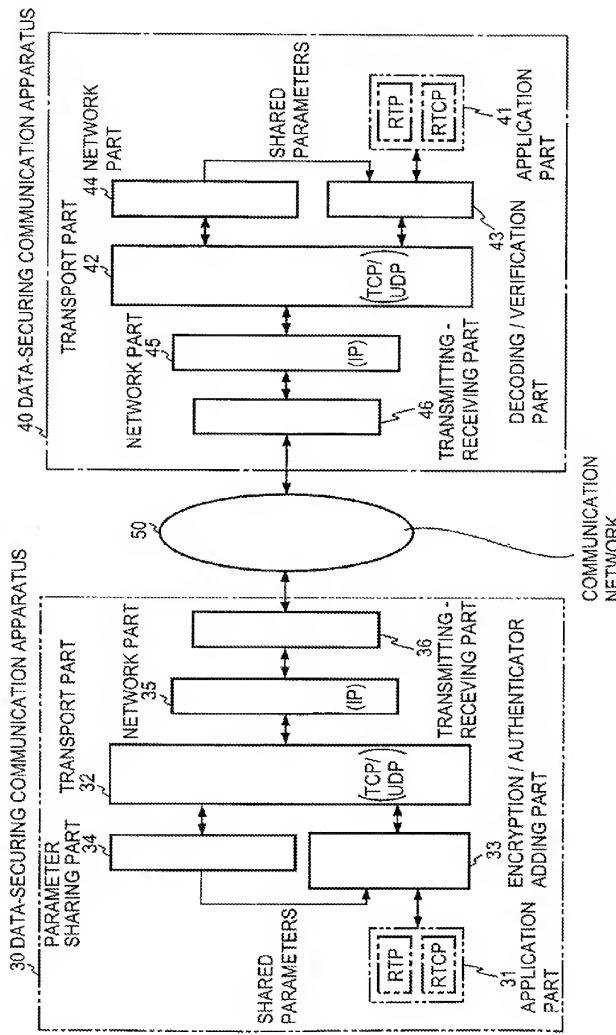


FIG.8

- ENCRYPTION ALGORITHM
 - Null, DES, 3DES, RC4, etc...
- DATA AUTHENTICATOR GENERATING ALGORITHM
 - MD5, SHA, etc...
- SECRET INFORMATION
- RANDOM VALUE
 - SERVER
 - CLIENT
- RANGE OF ENCRYPTION
- RANGE OF DATA AUTHENTICATION

FIG.9

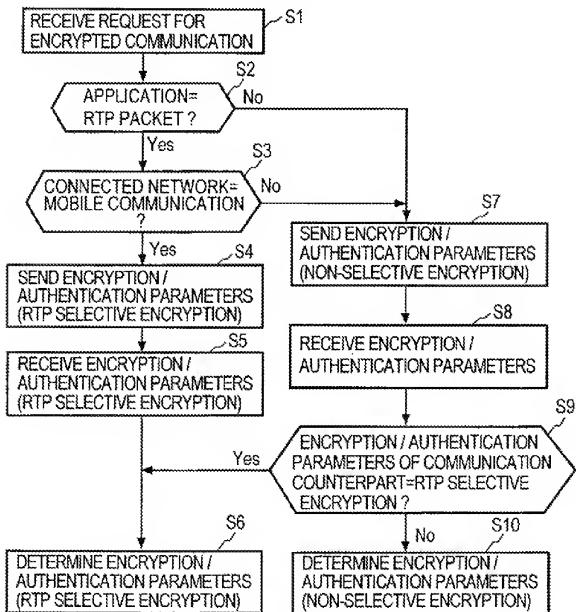


FIG.10

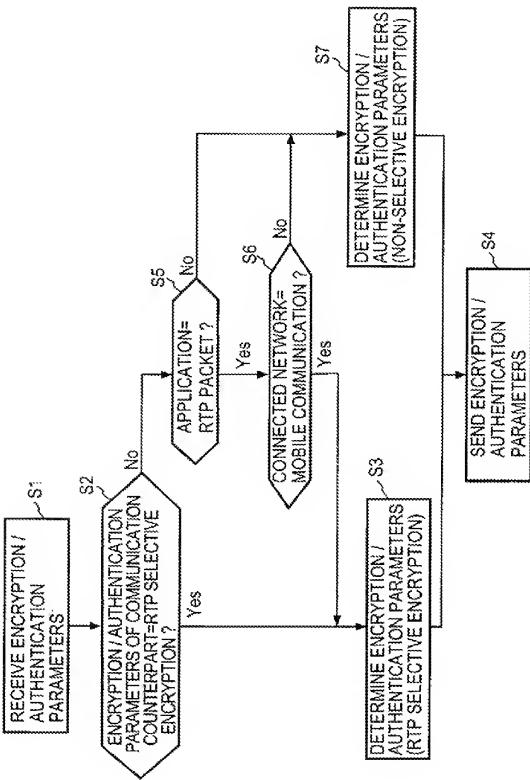


FIG.11

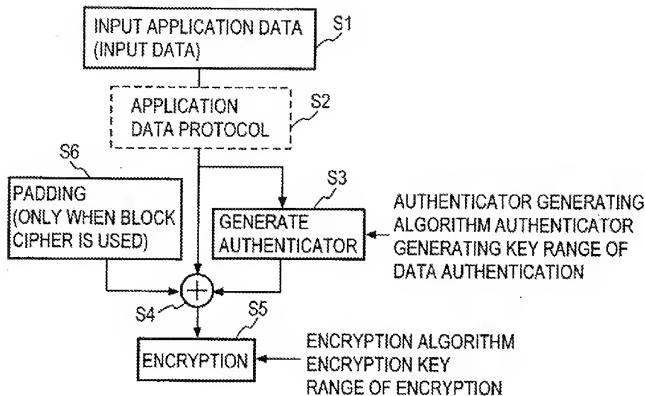


FIG.12

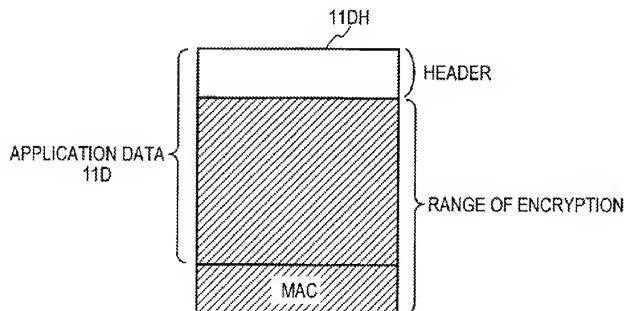


FIG.13

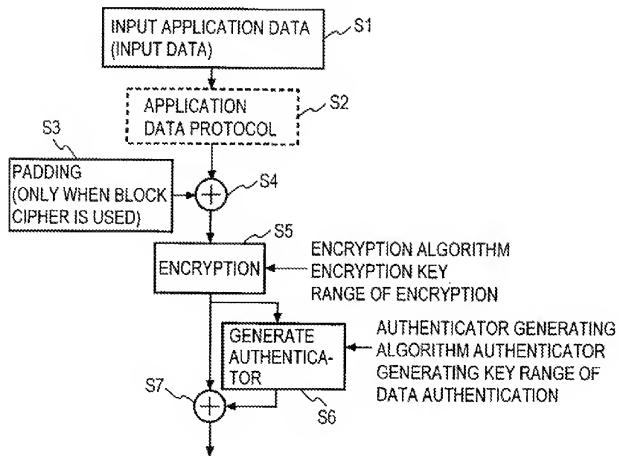
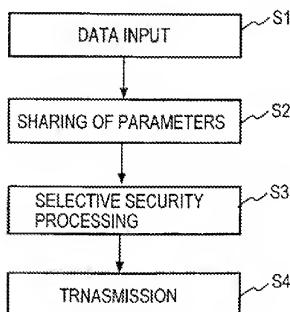


FIG.14



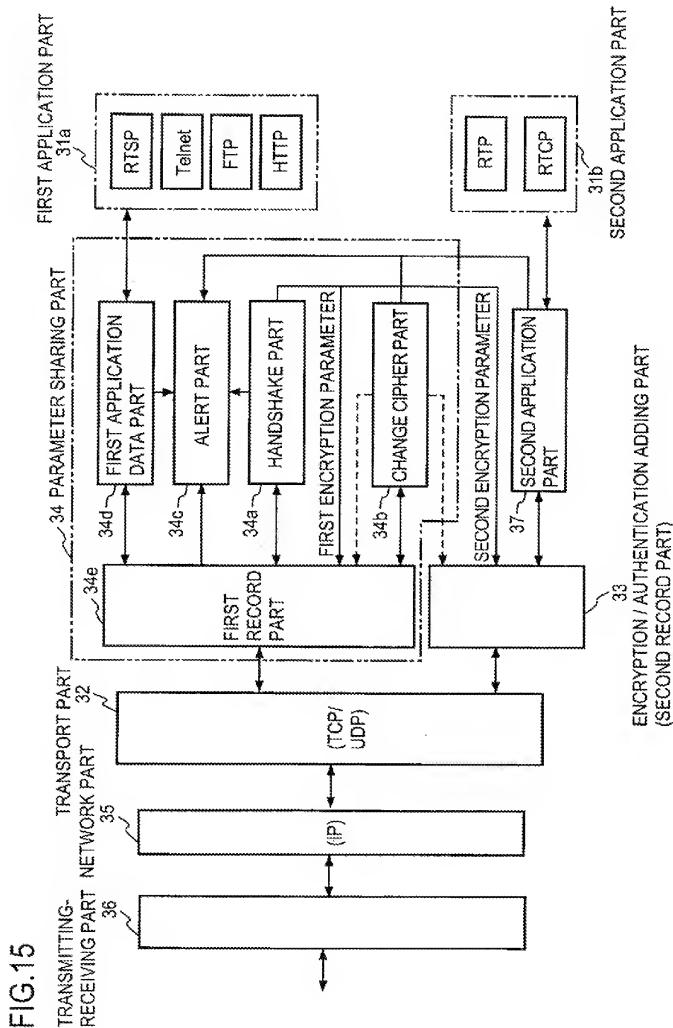
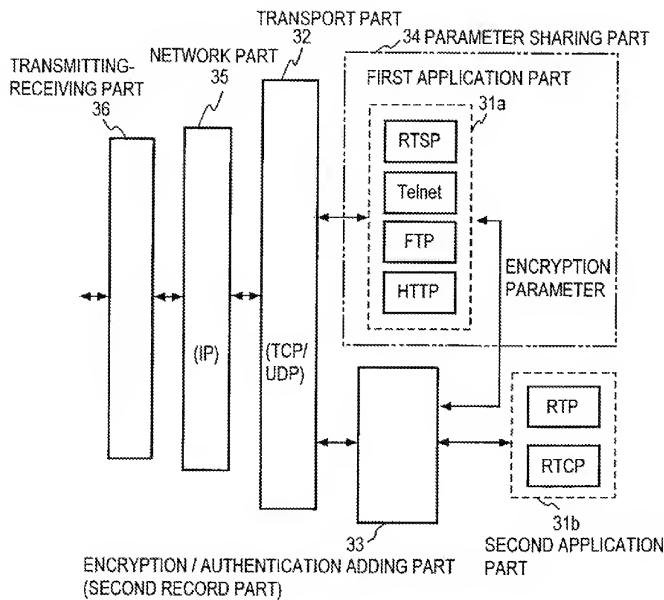


FIG.16



**DATA SECURING COMMUNICATION APPARATUS
AND METHOD****TECHNICAL FIELD**

[0001] The present invention relates to communication apparatus and method that provide data security against eavesdropping and falsification by encryption and authentication of the transmission data.

PRIOR ART

[0002] IP (Internet Protocol) networks, typified by the Internet, are not inherently equipped with security features. If no prevention measures are taken, it would be possible to eavesdrop and modify the contents of communication without arousing the notice of the parties concerned with the communication by the acquisition or alteration of the IP packet during transmission. Therefore, security protection is crucial for the transmission and reception of important information about business transactions or the like on the IP network.

[0003] For example, in content delivery services that deliver music and video through the Internet, the music and video data to be delivered are valuable important information and need to be protected against interception and falsification during transmission. And, in the VoIP system that offers telephone services through the IP network, it is necessary to prevent illegal eavesdropping of the contents of communication.

[0004] In the VoIP system and in a streaming content delivery system, RTP/UDP is commonly used as shown in FIG. 1A for the transmission of data required to be real-time. RTP (Real time Transport Protocol) is a protocol that is used in an application layer 11 and is suitable for real-time processing. UDP (User Datagram Protocol) is a connectionless protocol that is used in a transport layer 12 which is an interface between the application layer 11 and a network layer 13.

[0005] A transmission packet according to this system comprises, for example, as shown in FIG. 2, an IP header 13H, a UDP header 12H, an RTP header 11H and an RTP payload 11PL. Since RTP/UDP is intended for real-time packet transmission rather than for ensuring packet transmission like TCP (Transmission Control Protocol, a connection-type protocol that is used in the transport layer), there is a possibility of the occurrence of a packet loss during transmission. For this reason, measures against the packet loss should be taken into account on the occasion of studying the security scheme for application to RTP/UDP.

[0006] Further, it is also important to apply security techniques to mobile communications now quickly spreading. For RTP/UDP packet transmission in a mobile communication network, headers of both of the RTP packet (RTP header+RTP payload) and the UDP packet (UDP header+RTP packet) compressed in a radio link with a view to improving the utilization efficiency of the radio transmission band. Accordingly, it is to be wished that the security scheme, especially, the encryption system be one that allows header expansion/compression of the RTP/UDP packet in links halfway through transmission.

[0007] As a secure RTP packet transmission system for application to mobile communication networks, Secure RTP

(SRTP, see: draft-ietf-avt-srp 60. txt) has been proposed by IETF (Internet Engineering Task Force). In SRTP there have been introduced a selective encryption system that allows header compression and an encryption system that lessens the influence of the packet loss or bit error. That is, the RTP packet is processed, as depicted in FIG. 3, by encrypting only the RTP payload 11PL, and generating and adding a data authentication code (authenticator) 11A to the encrypted RTP payload 11PL and the RTP header 11H so that the validity of data of the RTP header 11H and the encrypted RTP payload 11PL can be verified. This technique permits efficient protection but RTP-specific.

[0008] That is, Secure RTP necessitates the use of an RTP-specific encryption algorithm and encryption parameter, and hence it cannot be utilized for applications and transport protocols other than UDP systems. Since its selective encryption parameter and encryption algorithm are fixed, Secure RTP cannot deal with new protocols and hence it is not suited to content delivery that makes rapid progress. A security technique specialized for a particular application, as mentioned above, is not preferable since it is necessary to study an individual security technique each time a new application is developed. Further, although the security technique is not permanent, Secure RTP has its encryption algorithm fixed and hence raises a problem in terms of security.

[0009] On the other hand, SSL (Secure Socket Layer) (TLS) is now widely used as a security technique on the Internet. When SSL (TLS) is not used, applications in layer 11, such as HTTP (Hypertext transfer Protocol), FIP (File Transfer protocol) and Telnet (remote log-in), are connected directly to a TCP or UDP transport layer 12 as shown in FIG. 4A. In contrast thereto, SSL is a security protocol that is located between the TCP or UDP transport layer 12 and the application layer 11 as depicted in FIG. 4B. SSL provides a secure data transmission service to the application layer by performing some security processing of data that is sent and received through utilization of the data transmission function offered by TCP or UDP. Therefore, there is no limitation to application and encryption algorithm to be utilized. SSL is in wide use particularly for an HTTP session in a Web access, but it can also be used versatilely for other applications of FTP and Telnet. Moreover, there is proposed, as a modified version of SSL for mobile communication use, WTLS (Wireless Transport Level Security) standardized in the WAP (Wireless Application Protocol) Forum.

[0010] SSL and WTLS generally have a two-layer configuration as depicted in FIG. 5. The protocol that is used in the lower layer 11S2 in the two-layer configuration is called Record Protocol, and it offers facilities for encrypting protocol data of the upper layer 11S1 and adding a data authentication code (MAC). The upper layer 11S1 in the two-layered configuration of SSL contains four kinds of protocols, a handshake protocol HSP (Handshake Protocol), an alert protocol ALP (Alert Protocol), a change cipher protocol CCP (Change cipher Protocol) and an application data protocol ADP (Application Data Protocol). The handshake protocol HSP possesses negotiation facility of an encryption/data authentication scheme and terminal/server authentication; the alert protocol ALP possesses an event and error indicating facility; and the change cipher protocol CCP possesses a facility of validating an negotiated encryp-

tion/authentication scheme. The application data protocol for indicating the state of encrypted communication to the other party is to transparently send and receive upper-layer application data; HTTP or FTP data in the application layer 11 is provided via this protocol to the record protocol (Record Protocol) 11S2.

[0011] FIG. 6 shows an example of the data configuration that is sent and received between record protocols (Record Protocols) of the sending and received sides. In a header 20f there are contained an identifier (Protocol type) 21 indicating the kinds of upper-layer protocols (such as handshake, alert and application data), an SSL version (Major Version, Minor Version) 22, and data lengths (Length (high), Length (low)) 23A and 23B. A payload 24 is encrypted upper-layer protocol data; the encrypted data 24 contains a data content (Content) 24A and an authenticator MAC 24B for verifying the validity of the data content and the header. This configuration is applied to all protocols that utilize the record protocol 11S2, including the application data protocol. Accordingly, in the case of transmitting the RTP packet by use of SSL, the header and the payload in their entirety are encrypted and mapped into the payload 24 of the record protocol data.

[0012] When the header of the record protocol is added to such an encrypted version of the whole RTP packet or the RTP packet, it is impossible to perform RTP header compression during transmission. That is, since the header compression is performed collectively for the RTP header, the UDP header and the IP header arranged one after another as depicted in FIG. 2, if a record protocol header 10 is inserted between the RTP header and the UDP header, they cannot collectively be data-compressed. For this reason, the application of SSL/WTLS to the RTP packet protection is not desirable in mobile communications.

[0013] In common data communications, too, it would be convenient if only a particular portion desired to protect could be secured by encryption or authentication for verification of its validity, but it has been difficult to adaptively provide security.

[0014] An object of the present invention is to provide a data-secur ing communication apparatus and method that permit communication with only part of input data selectively secured.

DISCLOSURE OF THE INVENTION

[0015] According to the present invention, the communication apparatus at the sending side shares parameters indicating a securing target of input data with a data-secur ing communication apparatus at the receiving side via a communication channel, and selectively secures part of the input data according to the shared parameter, thereafter outputting the data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] FIG. 1A is a diagram showing processing that does not use Secure RTP.

[0017] FIG. 1B is a diagram showing processing that uses Secure RTP.

[0018] FIG. 2 is a diagram depicting an example of packet configuration.

[0019] FIG. 3 is a diagram depicting data configuration of a selectively encrypted packet.

[0020] FIG. 4A is a diagram showing application data processing that does not use SSL/WTLS.

[0021] FIG. 4B is a diagram showing application data processing that uses SSL/WTLS.

[0022] FIG. 5 is a diagram showing particulars of the SSL/WTLS layer.

[0023] FIG. 6 is a diagram showing the configuration of record protocol data processing by SSL/WTLS.

[0024] FIG. 7 is a diagram illustrating the functional configuration of an embodiment of this invention apparatus and an example of the system configuration in which this invention apparatus is used.

[0025] FIG. 8 is a diagram showing examples of encryption parameters.

[0026] FIG. 9 is a flowchart showing an example of an encryption range sharing procedure at the transmitting side.

[0027] FIG. 10 is a flowchart showing an example of an encryption range sharing procedure at the receiving side.

[0028] FIG. 11 is a flowchart showing an example of the procedure of an encryption/authenticator adding part 33 in FIG. 7.

[0029] FIG. 12 is a diagram depicting an example of the data configuration of the output packet from the encryption/authenticator adding part 33.

[0030] FIG. 13 is a flowchart showing another example of the procedure of the encryption/authenticator adding part 33.

[0031] FIG. 14 is a flowchart showing an example of procedure of this invention method.

[0032] FIG. 15 is a diagram illustrating the functional configuration of a second embodiment of this invention apparatus.

[0033] FIG. 16 is a diagram illustrating the functional configuration of a third embodiment of this invention apparatus.

BEST MODE FOR CARRYING OUT THE INVENTION

[0034] FIRST EMBODIMENT

[0035] FIG. 7 illustrates a first embodiment of the present invention and the general outline of a data transmission system using the embodiment.

[0036] A data-secur ing communication apparatus 30 of the present invention, for example, at such a transmitting side as a server or data terminal and a data-secur ing communication apparatus 40 of the present invention similarly at such a receiving side as a server or data terminal can be connected via a communication network 50. The communication network 50 is shown as one network, but it may also be formed by plural networks such as a combination of a public communication network and the Internet.

[0037] The data-secur ing communication apparatus 30 in this embodiment has, as securing means, an encryption/authenticator adding part 33 between an application part 31

and a transport part 32. And, a parameter sharing part 34 is provided as an upper layer of the transport part 32. The transport part 32 has a TCP or UDP function and is connected, for example, to a network part 35 equipped with an IP function, and the network part 35 is connected to a transmitting-receiving part 36 that is a physical layer, and the transmitting-receiving part 36 is connected to the communication network 50.

[0038] The data-securing communication apparatus 40 is substantially identical in configuration with the data-securing communication apparatus 30; that is, it is provided with an application part 41, a transport part 42, a network part 45 and a transmitting-receiving part 46, and in this embodiment, a decoding/verification part 43 is provide as securing means, and a parameter sharing part 44 is provided as an upper layer of the transport part 42.

[0039] Prior to the transmission of application data from the application part 31, the communication apparatus 30 negotiates with the counterpart apparatus 40 about parameters necessary for data security that is, parameters necessary for encryption processing/decryption authenticator (code) generation processing, and shares those parameters with the counter part apparatus 40. The parameters are: information for specifying which of algorithms Null, DES, 3DES, RC4 and so on is used; secret information for key generation; random values for encryption/decryption or authentication/verification in the communication apparatus 30 (for example, a server apparatus) and the communication apparatus 40 (for example, a client apparatus); the range over which to encrypt transmission data; and the range of data authentication.

[0040] In this embodiment it is particularly important that the parameters for specifying the range of encryption and the range of data authentication are newly provided as shared parameters, and the other parameters are shared in the same way as that for shared parameters used in securing protocols by conventional SSL (TSL) scheme; sharing of these parameters is performed by intercommunication between the communication apparatuses 30 and 40 via the communication channel as is the case with conventional SSL scheme.

[0041] In this case, the newly shared parameters which indicate the securing target of data to be transmitted—the range of encryption and the range of data authentication in this example—are information for determining the range over which it encrypt and authenticate the input data packet (data packet from the application part 31 in this example), and various methods are possible for specifying the range; for example, information “start encryption at such and such a byte from the beginning of the packet” is used to specify the range.

[0042] Further, the range of encryption and the range of data authentication are determined according to the kind of input data, that is, the application in this example, or according to the transmission characteristics (such as the transmission rate, delay characteristic, transmission error characteristic, attenuation characteristic, frequency characteristic and distortion characteristic) of the communication network 50 to which the communication apparatus 30 is connected.

[0043] The parameter sharing part 34 of the communication apparatus 30 determines sharing of the parameters

indicative of the securing target, for example, by the procedure shown in FIG. 9. On receiving a request for encrypted communication (S1), the parameter sharing part makes a check to see if the input data application packet is an RTP packet (S2); if it is an RTP packet, makes a check to see if the communication network 50 to which the apparatus 30 is connected is a network of low transmission rate, for example, a mobile communication network (S3); and if it is a mobile communication network, transmits to the other communication apparatus 40 encryption/authentication parameters indicating selective encryption of the RTP packet (indicating, for example, that the RTP header at the beginning of the input data is excluded from encryption) (S4). At this time, other parameters, such as the encryption algorithm and the data authenticator generation algorithm, are also sent.

[0044] On the other hand, upon receiving the encryption/authentication parameters from the communication apparatus 30 (S1) as shown, for example, in FIG. 10, the parameter sharing part 44 of the communication apparatus 40 makes a check to see if the received encryption/authentication parameters are those for selective encryption of the RTP packet (S2); if so, determines that the encryption/authentication parameters in the parameter sharing part 44 are those for RTP packet selective encryption (S3); and sends the determined encryption/authentication parameters to the communication apparatus 30 (S4).

[0045] On receiving from the communication apparatus 40 the encryption/authentication parameters indicating RTP packet selective encryption (S5) as shown in FIG. 9, the parameter sharing part 34 of the communication apparatus 30 determines the encryption/authentication parameters as the target of RTP packet selective encryption (S6). In this way, the both parameter sharing parts 34 and 44 share the RTP selective encryption as the encryption/authentication parameters via the communication channel. Incidentally, the encryption algorithm and other parameters are similarly determined at the same time. In this instance, as is the case with conventional SSL, for instance, several candidates for each parameter are sent to the apparatus 40 for determination.

[0046] In FIG. 9, when it is decided in step S2 that the input data is not an RTP packet, or when it is decided in step S3 that the transmission rate of the communication network 50, to which the communication apparatus 30 is connected, is high, the communication apparatus sends to the counterpart 40 encryption/authentication parameters indicating encryption of the whole input data (packet), that is, indicating non-selective encryption (S7).

[0047] As depicted in FIG. 10, when it is decided in step S2 that the encryption/authentication parameters are not for RTP packet selective encryption, the parameter sharing part 44 of the communication apparatus 40 decides whether the input data (application) from the application part 41 of the communication apparatus 40 is an RTP packet (S5); if it is an RTP packet, makes a check to see if the communication network 50 to which the communication apparatus 40 is connected is, for example, a mobile communication network of low transmission rate (S6); and if so, goes to step S3, in which it determines the encryption/authentication parameters indicating RTP packet selective encryption and sends it to the communication apparatus 30 (S4). When it is decided

in step S5 that the input data is not an RTP packet, or when it is decided in step S6 that the communication network 50 is not a mobile communication network whose transmission rate is not low (S6), the parameter sharing part determines encryption/authentication parameters indicating non-selective encryption (S7), and sends the parameters to the communication apparatus 30 (S4).

[0048] As depicted in FIG. 9, upon receiving the encryption/authentication parameters from the communication apparatus 40 (S8) after the transmission in step S7, the parameter sharing part 34 of the communication apparatus 30 makes a check to see if the received encryption/authentication parameters are those for RTP packet selective encryption (S9); if so, goes to step S6, in which the parameter sharing part determines the encryption/authentication parameters as those for RTP packet selective encryption; and if not for RTP packet selective encryption, determines the encryption/authentication parameters as those for non-selective encryption (S10).

[0049] In this way, the parameter sharing parts 34 and 44 can share the range of encryption via the communication channel. The range of authentication is set to be the whole input data irrespective of the input data (application) and independently of the transmission characteristic of the communication network 50 to which the communication apparatuses 30 and 40 are connected. The range of encryption can be specified not only as to whether to exclude the header from encryption but also as desired. For example, when the input data is image or audio data, it is also possible to limit the range of authentication specifically to an important portion which, if lost would make decoding impossible. In either case, the encryption algorithm and other parameters are also subjected to sharing processing simultaneously with sharing of the range of encryption.

[0050] When the parameters are shared as described above, they are provided to the encryption/authenticator adding part 33 and the decoding/verification part 43 from the parameter sharing parts 34 and 44, respectively.

[0051] The encryption/authenticator adding part 33 performs encryption/authenticator adding processing. An example of the procedure thereof is shown in FIG. 11. When input from the upper application part 31 (S1), a data packet is transparently input to the encryption/authenticator adding part 33 by an application data protocol (S2), and an authenticator is generated by a shared authenticator generating algorithm/authenticator generating key by use of that portion of the data packet selected according to the authentication range parameter (S3). The authenticator generating method is described in detail, for example, in IMAI Hideki, "Lecture on Cryptography," Section 4.7. The authenticator is generated, for instance, by compressing the authentication range data by a hash function and encrypting the compressed data by the common key. Then the authenticator is added to the input data packet (S4), and that part of the authenticator-added data packet which is selected based on the encryption range parameter is encrypted using the shared encryption algorithm and encryption key (S5). Incidentally, in the case of block encryption, padding is carried out prior to the encryption in anticipation of the shortage of data for the fixed block length (S6).

[0052] In FIG. 12 there is shown an example of the configuration of such encrypted data. In this example the

authenticator MAC is added to the input application data 11D, and the portion (payload) of the application data, except the header 11D1, and the authenticator MAC are encrypted. The selectively encrypted data is provided to the lower transport part 32, from which it is sent to the other communication apparatus 40.

[0053] The receiving-side communication apparatus 40 decodes the encrypted data following the procedure reverse to that described above, and the validity of the received data is verified by use of the data authenticator (code). That is, in the communication apparatus 40 in FIG. 7, the packet received from the communication apparatus 30 is input from the transport part 42 to the decoding/verification part 43, and in the decoding/verification part 43 the encrypted portion is selectively decoded according to the shared encryption algorithm, encryption key and range of encryption, and the data authenticator (code) MAC in the decoded data is used to verify the validity of the header and the decoded payload, that is, the application data in FIG. 12. The application data, if valid, is supplied to the application part 41.

[0054] By such sharing of the range of encryption, it is possible to selectively encrypt part of the input data; for example, encryption of only that portion of the input data whose security becomes an issue makes the workload lighter than in the case of encrypting the whole input data, and settles the security issue. The range of encryption can be shared simultaneously with sharing of the other parameters for encryption, and an increase in the workload therefor is very slight.

[0055] In particular, when the input data (application) is an RTP packet as mentioned above, if the header portion of the RTP packet is not encrypted, a UDP packet header and an IP packet header are added to the above header—this provides for header compression, including the RTP packet, during transmission as is the case with Secure RTP. Further, since the area of encryption can be set at the beginning of the session through negotiations with the receiving side unlike in the case of Secure RTP, this scheme can also be applied versatilely to other applications than the RTP packet.

[0056] Although in FIG. 11 the addition of the authenticator is followed by encryption, it is also possible to generate the authenticator after encryption (S5) and add the authenticator to the encrypted packet (S7) as depicted in FIG. 13. In this case, at the receiving side the verification of the validity of the received data is followed by decoding. When padding (S3) is necessary, it precedes encryption (S5).

[0057] The flow of the above-described selective security processing is shown in FIG. 14, in which, upon input thereto of data (S1), the transmitting-side communication apparatus shares parameters indicative of the securing target of the input data with the receiving-side communication apparatus via the communication channel (S2); perform security processing of part of the input data based on the shared securing target parameters (S3); and transmits the input data (S4).

[0058] SECOND EMBODIMENT

[0059] FIG. 15 illustrates a second embodiment of the present invention. This embodiment is adapted to be capable of supporting the selective encryption by extending the SSL scheme depicted in FIG. 5. The parameter sharing part 34 in the first embodiment further comprises: a handshake (Handshake) part 34a for negotiating with the receiving-side

communication apparatus **40** about authentication processing and encryption/data authentication parameters; a change cipher (Change Cipher) part **34b** for validating the encryption/data authentication parameters; an alert (Alert) part **34c** for indicating an event/error; a first application data part **34d** for transparently sending and receiving upper-layer application data; and a first record (Record) part **34e** for sending and receiving protocols of the above-mentioned three parts **34a**, **34b**, **34c** and **34d** via the lower layer part (transport part) **32**.

[0060] The first record part **34e** uses, as its protocol data format, the same format as that of the SSL record part shown in FIG. 6. The shake-hand part **34a** negotiates with the receiving-side communication apparatus **40** about the encryption/data authentication parameters that are used in the first record part **34b** and the second record part (encryption/authenticator adding part) **33**. And the change cipher (Change Cipher) part **34c** validates the encryption/data authentication parameters of the first record part **34e** and the second record part **33**. That is, it starts and indicates encryption to the receiving side. To the first record application data part **34e** are input a protocol message of the handshake part **34a** and application data that does not necessitate the selective encryption in the first application data part **34d**.

[0061] The transmission and reception of application data that necessitates selective encryption are performed, independently of the above-mentioned protocol data, by a second record part, that is, by the encryption/authenticator adding part **33**. A second application data **37** is to transparently send and receive the data packet of a high-order second application part **31b** to and from the second record part **33**. Further, unlike the first record part **34e** the second record part, that is, the encryption/authenticator adding part **33** does not add a new header to the input data but performs the encryption/authenticator generation processing alone. The parameters shared by the first record part **34e** are used for the encryption/data authentication processing in the second record part **33**. The encryption/data authentication processing is the same as in the first embodiment.

[0062] The handshake part **34a** starts the parameter sharing procedure using plaintext communication with the receiving-side communication apparatus **40**, and may protect the communication using shared encryption/authentication parameters halfway through the procedure among applications an application data packet which is not required to have the real time property and is not frequently sent, such as HTTP, FTP, Telnet or RTSP (a protocol for opening the RTP session), is input from a first application part **31a** via the first application data part **34d** to the first record part **34e**, which encrypts the input packet in its entirety based on the shared parameters and adds the encrypted packet with the header **20H** of the record part as depicted in FIG. 6, thereafter providing the packet as a record protocol packet to the transport part **32**. Incidentally, the receiving-side communication apparatus **40** has the same construction as depicted in FIG. 15 except that the encryption/authenticator adding part **33**, which is the second record part, is a decoding/verification part.

[0063] THIRD EMBODIMENT

[0064] FIG. 16 illustrates a third embodiment of the present invention. This embodiment negotiates with the receiving-side via the first application part **31a** as of RTSP

or HTTP to share the encryption/authenticator adding parameter that are applied to the application data of the second application part **31b**. For example, encryption parameters in FIG. 8 can be transmitted to the receiving-side apparatus **40** by encrypting them by the public key of the receiving-side communication apparatus **40** and embedding the encrypted parameters in the protocol message body.

[0065] It is also possible to provide both of the encryption/authenticator adding part and the decoding/verification part in one communication apparatus. While the above embodiment performs, for data security, both of encryption and data authenticator addition, only one of them may also be utilized. The respective parts of the communication apparatuses **30** and **40** may be implemented by executing programs on a computer.

EFFECT OF THE INVENTION

[0066] As described above, the present invention provides security for a selected portion of data, permits versatile transmission data protection unspecific to a particular application, and enables header compression when employed in mobile communications in particular.

What is claimed is:

1. A data-securig communication apparatus comprising:
parameter sharing means for sharing parameters indicative of a securing target of input data with a receiving-side data-securig communication apparatus via a communication channel; and
securing means for selectively securing a portion of said input data based on said shared parameters.
2. The data-securig communication apparatus as claimed in claim 1, which is further provided with means for determining said securing target in accordance with the kind (application) of the input data.
3. The data-securig communication apparatus as claimed in claim 1 or 2, which is further provided with means for determining said securing target in accordance with the network to which said apparatus is connected.
4. The data-securig communication apparatus as claimed in any one of claims 1, 2, and 3, wherein said securing target is a target for encryption, said receiving-side communication apparatus being a decoding apparatus and said securing means being encryption means.
5. The data-securig communication apparatus as claimed in claim 4, wherein said input data is an RTP packet and said target for encryption is data except an RTP header.
6. The data-securig communication apparatus as claimed in claim 4, wherein the criterion for determining said target for encryption is the transmission rate of the communication channel of said network.
7. The data-securig communication apparatus as claimed in any one of claims 1, 2 and 3, wherein: said securing target is the range of authentication of said input data; said receiving-side data-securig communication apparatus is a data verification apparatus; said securing means is means for calculating an authenticator from said range of authentication of said input data; and means for outputting the input data after adding thereto said authenticator.
8. A data-securig communication apparatus comprising:
parameter sharing means for sharing parameters indicative of a decoding target of received data with a

transmitting-side data-securing communication apparatus via a communication channel; and decoding means for selectively decoding a portion of said received data based on said shared parameters.

9. A data-securing communication apparatus comprising:
(a) means for sharing parameters indicative of the range of authentication of received data with authenticator adding device of a transmitting side via a communication channel; and
verification means for verifying the validity of data contained in said range of authentication of the received data by data about said range of authentication and an authenticator contained in said received data according to said parameters.

10. A data-securing communication method comprising the steps of:
(a) sharing parameters indicative of a target for encryption of input data with a data decoding apparatus of a receiving side via a communication channel; and
(b) selectively encrypting a portion of said input data based on said shared parameters and outputting the selectively encrypted data.

11. The data-securing communication method as claimed in claim 10, wherein said input data is an RTP packet and said selective encryption is performed for data except an RTP header of said RTP packet.

12. A data-securing communication method comprising the steps of:
(a) sharing parameters indicative of the range of authentication of input data with a data verification apparatus via a communication channel;

(b) calculating an authenticator from that portion of said input data which is specified by said parameters; and
(c) outputting said input data after adding thereto said authenticator.

13. A data-securing communication method comprising the steps of:
(a) sharing parameters indicative of a decoding target of received data with an encryption apparatus of a transmitting side via a communication channel; and
(b) selectively decoding a portion of the received data based on said shared parameters.

14. The method as claimed in claim 13, wherein said received data is an RTP packet and said selective decoding is performed for data except an RTP header of said RTP packet.

15. A data-securing communication apparatus comprising the steps of:
(a) sharing parameters indicative of the range of authentication of received data with authenticator adding device of a transmitting side via a communication channel; and
(b) verifying the validity of data contained in said range of authentication of the received data by data about said range of authentication and an authenticator contained in said received data according to said parameters.

* * * * *